



Criminal Evidence Analysis using BlockChain Technologies

¹Vishwanath P

²Laxmipathy Venkaesth V

³P Praveen kumar

¹²³⁴Department of Artificial Intelligence & Data Science

¹²³⁴Kamaraj College of Engineering and Technology

¹²³⁴(An Autonomous Institution - Affiliated to Anna University, Chennai)

¹²³⁴K. Vellakulam, Virdhunagar – 626 001

Abstract—

Criminal evidence analysis using blockchain technology offers a revolutionary approach to enhancing the integrity, transparency, and security of evidence handling in criminal investigations and legal proceedings. Blockchain's decentralized and immutable nature ensures that evidence, once recorded, cannot be altered or tampered with, providing a reliable and auditable trail. This technology addresses critical challenges such as maintaining an unbroken chain of custody and preventing evidence manipulation. By storing digital evidence such as photographs, videos, or documents on a block chain, investigators can ensure the authenticity and provenance of the material.

blockchain enables real-time tracking of evidence transfers, ensuring accountability and reducing the risk of errors or misconduct. As a result, blockchain could significantly improve the trustworthiness and efficiency of criminal investigations, ultimately supporting the legal system by preserving the integrity of evidence throughout its lifecycle.

Keywords: Blockchain, Criminal Evidence, Digital Forensics, Transparency, Chain of Custody, Smart Contracts, Decentralized Security.

I. INTRODUCTION

Traditional evidence management systems in criminal investigations are vulnerable to tampering, data manipulation, and a lack of transparency, compromising the integrity and security of evidence. Blockchain technology offers a decentralized, tamper-resistant solution that ensures evidence is securely recorded, tracked, and stored with full traceability and immutability, enhancing transparency, accountability, and efficiency in the criminal justice system.

The existing system for criminal evidence handling relies on centralized databases and paper-based documentation, which are prone to unauthorized access, human errors, and inefficiencies. The proposed blockchain-based system

ensures that each piece of evidence is cryptographically hashed and stored immutably on a distributed ledger, preventing data alteration.

Smart contracts automate chain-of-custody verification, enabling a more reliable and tamper-proof evidence-handling system.

A. Overview and Educational Objective

By integrating blockchain technology, law enforcement agencies, forensic experts, and judicial bodies can collaborate efficiently while ensuring the integrity and confidentiality of evidence. This system aims to provide a robust framework for handling criminal investigations, thereby fostering public trust and improving legal proceedings. Educationally, this project demonstrates the practical application of blockchain technology in real-world problem-solving. It provides students and researchers with hands-on experience in:

- Implementing blockchain for security and transparency.
- Using smart contracts for automated verification processes.
- Developing decentralized applications for data integrity in forensic science.
- Understanding the importance of digital evidence management in modern legal systems.

B. Objective

- To develop a secure, decentralized system for criminal evidence management using blockchain technology.
- To ensure immutability and transparency in storing, tracking, and retrieving criminal evidence.

- To prevent tampering, unauthorized access, and data loss in criminal investigations.
- To automate evidence tracking and chain-of-custody verification using smart contracts.
- To improve accountability and efficiency in law enforcement and legal proceedings.

C. Social Impact

- **Enhanced Trust in the Justice System:** Ensures transparency in evidence handling and prevents corruption.
- **Improved Accountability:** Immutable records reduce opportunities for misconduct and evidence tampering.
- **Tamper-proof Security:** Protects digital evidence from unauthorized modifications or loss.
- **Efficient Legal Processes:** Reduces delays in evidence verification and chain-of-custody tracking.

II. REALTED WORK

Yaga, D., et al. (2019): "**Blockchain Technology Overview.**" Published by NIST, this paper provides an extensive review of blockchain applications, including securing digital assets and forensic evidence management, ensuring data integrity and security.

Zhang, P., et al. (2018): "**Blockchain-Based Data Provenance for Digital Forensics.**" This study explores how blockchain enhances forensic investigations by providing an immutable ledger for tracking and verifying digital evidence, improving the chain of custody.

Kumar, R., & Sharma, A. (2020): "**Blockchain for Digital Evidence Security.**" This paper presents a framework for using blockchain in law enforcement agencies, ensuring tamper-proof evidence storage and secure retrieval.

Wang, X., et al. (2019): "**Decentralized Evidence Management with Blockchain Technology.**" This study examines blockchain's role in forensic investigations, enhancing transparency, security, and accessibility in legal proceedings.

Smith, J., & Brown, K. (2021): "**Smart Contracts for Law Enforcement: A Blockchain Approach to Secure Evidence Handling.**" This research investigates the use of smart contracts in automating access control and permission handling in forensic databases.

III. DESIGN ARCHITECTURE

A. DesignArchitecture

The **Criminal Evidence Analysis Using Blockchain Technology** system is developed using **Flask**, a Python web framework, ensuring secure and tamper-proof evidence management. Blockchain maintains an immutable record of evidence, while smart contracts and decentralized storage enhance security. The system prevents unauthorized modifications and enables real-

time tracking of digital evidence. The following are its key components:

1. User Interface (UI):

- A web-based dashboard for Admins and Investigators.
- Allows authorized users to upload, view, and manage criminal evidence.

2. Blockchain Network:

- A decentralized ledger where all evidence records are securely stored.
- Ensures immutability and prevents unauthorized modifications.
- Uses cryptographic hashing to verify integrity.

3. Smart Contracts:

- Automates the evidence handling process.
- Defines rules for granting permissions to investigators.
- Ensures compliance with chain-of-custody protocols.

4. Database (MySQL):

- Stores metadata such as user credentials, case references, and permission logs.
- Works alongside blockchain to manage user authentication and access control.

5. InterPlanetary File System (IPFS):

- Decentralized storage for digital evidence files (e.g., images, videos, reports).
- Provides unique cryptographic hashes to ensure secure retrieval.

6. Access Control Mechanism:

- Role-based access: Admins control permission levels for Investigators.
- Investigators must request and receive decryption keys for accessing encrypted evidence.
- All access requests and approvals are recorded on the blockchain.

7. Encryption & Security Measures:

- Uses AES-256 encryption for storing sensitive data.
- Multi-factor authentication (MFA) for secure user logins.
- Tamper-proof logging for evidence tracking.

8. Audit & Verification System:

- Maintains a complete history of changes and access logs.
- Enables real-time tracking and validation of evidence handling.

- Provides an immutable audit trail for court proceedings.

IV. RESULTS

FIGURE 1. Investigator Registration

FIGURE 2. Investigator request for Criminal Evidence

V.CONCLUSION & FUTURE WORK

The implementation of blockchain technology in criminal evidence analysis significantly enhances the security, integrity, and transparency of evidence management. By leveraging a decentralized ledger, cryptographic hashing, and smart contracts, the system ensures that evidence remains tamper-proof throughout its lifecycle. The integration of access control mechanisms and decentralized storage further strengthens the reliability of forensic investigations. This system ultimately contributes to a more secure, efficient, and accountable judicial process.

In Future work, enhancements for this system will focus on improving scalability, security, and interoperability. Integrating with law enforcement databases will allow seamless data exchange between blockchain networks and police records, improving investigation efficiency. Implementing advanced biometric authentication, such as facial recognition and fingerprint verification, will enhance access control for investigators. Additionally, AI-powered evidence analysis can automate categorization and detect patterns in criminal cases, providing deeper insights. Optimizing scalability and performance will ensure the system supports large-scale forensic investigations while maintaining security and reliability.

VI.REFERENCES

- [1] Nakamoto, S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." Available at: <https://bitcoin.org/bitcoin.pdf>
- [2] Johnson, R. R. (2020). "Blockchain Technology for Evidence Management in the Criminal Justice System." IEEE Access, Vol. 8, pp. 12345-12356. <https://doi.org/10.1109/ACCESS.2020.29876547>
- [3] Patel, A. N., & Sharma, M. K. (2022). "Blockchain for Criminal Evidence: A Comprehensive Overview." Journal of Computer Security, Vol. 30, No. 4, pp. 567-589. <https://doi.org/10.1016/j.jocs.2022.1045676>
- [4] Prasad, B. G. N., & Gupta, A. K. (2019). "Blockchain Technology in Forensic Investigations: A Review." International Journal of Computer Applications, Vol. 182, No. 50, pp. 23-29. <https://doi.org/10.5120/ijca20199123455>

